REMARKS

In the first Office Action, the Examiner rejected claims 1-86 under the judicially created doctrine of obviousness-type double patenting based on a number of commonly owned pending applications and issued patents. The Examiner rejected claims 1-86 under 35 USC §102(b) as being anticipated by Ananda (US 5,495,411).

While Applicant does not agree with the double patenting rejection, due to the number of pending claims and the number of references alleged to render the claims unpatentable, Applicant submits herewith a terminal disclaimer to obviate the double patenting rejection.

Applicant respectfully disagrees with the Examiner's rejection under 35 USC §102(b) based on Ananda (US5,495,411) and traverses the rejection for the reasons described in detail below.

Reconsideration and re-examination of the application considering the following remarks is respectfully requested.

Information Disclosure Statements

The Examiner is respectfully requested to consider the documents and initial the Information Disclosure Statements filed on 9/20/06 relative to litigation of related U.S. patents. These Information Disclosure Statements were not included with the Office Action mailed to Applicant on 11/21/06.

Double Patenting

The Examiner rejected claims 1-86 for obviousness-type double patenting. While Applicant does not agree with the Examiner's position, Applicant submits herewith a Terminal Disclaimer to obviate the Examiner's rejection and advance the prosecution of this case.

Rejection Under 35 USC §102(b)

The Examiner rejected claims 1-86 as being anticipated by Ananda (US 5,495,411). Applicant respectfully disagrees and traverses the Examiner's rejection.

A rejection for anticipation requires that each and every element of Applicant's claims be disclosed explicitly or inherently in a single reference. As described in greater detail below, Applicant's claims include a number of features that are not disclosed in Ananda '411, and Applicant respectfully requests the Examiner to reconsider and withdraw the rejection.

Summary of Ananda '411

The '411 reference cited by the Examiner is directed to a software rental system using continuous password verification. The system allows a remote user computer system 150 to use application software downloaded from a central rental facility 180 only while the remote user computer system 150 is electronically connected to the central rental facility. This is accomplished by attaching additional header software 320 (Fig. 3) to the application software 310. Header software 320 includes a rental security manager 321 having modules for authorization verification 321A, execution termination 321B, encryption/decryption 321C, message processor 321D, password generation 321E, and password validation 321F.

During operation, a user provides a user identification password to access the central rental facility 122 (and remote computer 180), which compares the user password to user identification information in registration database 212 to determine if the user password is authorized (Col. 8, ll. 7-38). The user then selects an application program from the rental application database 214. In response, multiuser controller 222 transfers the selected application software 310 and header software 320 through modem 126 to the remote user computer system 150 (Col. 8, ll. 54-64). Central rental facility 122 records the processor clock time of the transfer and an application ID in a file for subsequent use in generating passwords, as well as sending an encrypted message with this information to the user computer system 150.

The rental security module 321 in the header software 320 on the user computer uses 1) the difference between the transfer time from the Central Rental Facility computer 180 and the local processor clock time, and 2) the user password entered to gain access to the Central Rental Facility, as input to a pseudorandom number generator to generate an authorization verification password that is associated with the software by an application ID number. The user computer clock time, user ID password, and authorization verification password are sent to the Central Rental Facility, which also uses 1) the difference between the stored transfer time and the current clock time of the user computer, and 2) the user ID password as input to a pseudorandom number generator that generates an authorization verification password, which is sent back to the Rental Security Module on the user computer. The authorization verification passwords are compared by the Rental Security Module 321 to determine if the SW is authorized. This process is repeated every 100 ms to ensure a continuous connection between the Central Rental Facility and the local user computer. If the authorization verification password comparison fails 3 times, execution of the application software program on the local user computer is terminated by termination module 321B (Col. 15, ll. 7-63).

Summary of Applicant's Claimed Invention

Applicant's invention as claimed in independent claims 1, 23, 46, and 75 is directed to a method for securing software to reduce unauthorized use that associates at least one identifier with the software to designate the software for protection by an authorized representative entity. The identifier feature of the invention is best illustrated in Figs. 62, 67, and 68 and described in Paras. [0291] and [0309] – [0314]. The identifier indicates that anti-piracy measures or copy protection is desired by the software distributor. The identifier may be in the form of a serial number, password, or other alphanumeric or binary string, for example and is preferably transparent to any systems that do not include an authorized representative or other module or device to implement copy protection so that the software may be used without restrictions on those systems or devices. As also described and illustrated in Figs. 67-68, the identifier may be included in a unique file prefis, file suffix, file extension, embedded within the content, or as a binary code, for example.

As illustrated and described with reference to Fig. 68, software that includes at least one identifier to trigger an authentication process on a user's system, network, or device is distributed to the user. The identifier is detected by an authorized representative entity that may be installed on or in the user device, and/or remotely located relative to the user device. The authorized representative entity then determines whether attempted access to the software is authorized based on registration information and/or an authentication code associated with the software. The registration information and authentication code(s) may be associated with a particular user device or a group of authorized devices.

Distinguishing Features of Applicant's Claimed Invention

Applicant's claimed invention includes a number of features that are not disclosed in Ananda. At least one feature or limitation in each of the following claims is not disclosed in Ananda. However, the following is not intended to be an exhaustive description and various other features and/or claims may include other distinguishing limitations that are not disclosed in Ananda and not explicitly described below.

In general, Ananda '411 does not disclose software with an identifier that triggers an authentication or authorization process as disclosed and claimed. The Examiner cites various passages from Ananda that relate to the header software and the incorporated rental security manager 321 that generate authorization verification passwords. However, it is not clear from the rejection how these features are being applied to various elements of Applicant's claims. It appears from the rejection of various claims that the Examiner's interpretation is necessarily inconsistent in rejecting an independent claim and its corresponding dependent claims. For example, it appears the Examiner is interpreting the header module as the identifier associated with the software, but also as the authorized representative entity that detects the identifier associated with the software in rejecting claim 1. This interpretation appears to change in the rejection of dependent claims 4-8 where the cited passages refer to the authorization verification password generated by the rental security manager, such that the Examiner is indicating that the authorization verification password is now the element that anticipates Applicant's claimed "identifier", which is improper.

The Examiner is respectfully requested to clarify the elements of Ananda that anticipate each element of Applicant's claims rather that reciting the entire claim followed by a citation to multiple columns/lines in Ananda that purportedly anticipate all the elements of the claim to facilitate Applicant's understanding and analysis of the Examiner's position. For example, Ananda discloses a user password that is associated with a registration database of user information, a header module that includes a rental security manager having modules to generate authorization verification passwords, perform encryption/decryption, terminate application execution, etc. The Examiner is respectfully requested to identify which of these elements is purported to anticipate Applicant's claimed identifier or plurality of identifiers, and which element anticipates the authorized representative entity that detects the identifier. Similarly, the Examiner is requested to identify which feature of Ananda anticipates Applicant's registration information associated with a user device.

With respect to claim 1, Ananda does not disclose associating at least one identifier with the software prior to distribution of the software that is detectable to request authentication of the software by an authorized representative, but allowing the software to function if not detected, and distributing the software with the identifier to a user. If the Examiner is interpreting the header module disclosed by Ananda as anticipating the "identifier" claimed by Applicant, the header module is not "detected" by the user computer, and can not function as or anticipate both the claimed "identifier" and the "authorized representative". If the Examiner alleges that the header module is detected as claimed, then it can not meet the limitations of Applicant's claim 8 that requires the module to be encrypted, claim 19, which requires that the identifier be included in a filename, claim 20 that requires it be a filename prefix, suffix, or extension, or claim 22 that requires it be hidden to the user. Alternatively, if the Examiner is interpreting the authorization verification password or user password disclosed by Ananda as the "identifier" claimed by Applicant, then it is not distributed with the software as required by claim 1, and is not detectable to request authentication of the software as claimed.

As per claim 2, Ananda does not disclose any feature that is self authenticating and self activating in conjunction with an authorized representative located on or in the user device as claimed. Ananda requires continuous communication with a remote authorized representative to generate authorization verification passwords and is therefore not self activating and self authenticating as disclosed and claimed by Applicant.

As per claim 6, the authorization verification message and the password it contains are not embedded within a file of the software as claimed. Ananda clearly states that the authorization verification password is generated after distribution of the software and therefore can not be embedded as claimed by Applicant, particularly since it relies on the transfer time of the software.

As per claim 8, the authorization verification password may be encrypted, but is not generated prior to distribution of the software as required. Similarly, the header module and/or rental security manager is associated prior to distribution, but is not encrypted. As such, neither meets Applicant's claim limitations.

As per claim 10, Ananda discloses distribution of the software via a telephone network and not via a computer readable storage medium as disclosed and claimed by Applicant.

As per claim 11, Ananda does not disclose any detection of an identifier to trigger authentication as disclosed and claimed by Applicant. The header module executes without regard to any identifier and therefore does not perform the authorization process based on detection of the at least on identifier as claimed.

As per claim 12, Ananda does not disclose registration information associated with the software. The only registration information disclosed by Ananda is contained in the registration database at the central rental facility and includes a user identification password, which is not associated with the software.

As per claim 13, the registration information disclosed by Ananda is not associated with a user device as claimed. Rather, the registration information is associated with the user upon initial access to the central rental facility.

As per claims 19-20, none of the registration information, header module, or authorization verification passwords disclosed by Ananda are included in a filename for a software component, and none are included as a filename prefix, suffix, or extension as claimed.

As per claim 23, Ananda does not disclose a plurality of identifiers associated with the software as claimed. In addition, Ananda requires continuous contact with the central rental facility, a remote authorized representative entity. Ananda does not disclose an identifier that is detectable by the authorized representative entity as claimed. If the Examiner interprets the authorization verification password as the "identifier", it is not associated with the software prior to distribution.

As per claim 24, the software disclosed by Ananda requires contact with a remote authorized representative at the central rental facility and is therefore not self activating and self authenticating with an <u>authorized representative located on or in the user device</u> as claimed.

As per claim 25, none of the features disclosed by Ananda, including the authorization verification passwords, the header module, and the rental security manager are entered by the user. If the Examiner interprets the user identification password entered to access the central rental facility as anticipating the "authentication code" that is one of the plurality of "identifiers" then it is not associated with the software prior to distribution, and is not detected to trigger authorization as claimed by Applicant.

As per claim 29, none of the features disclosed by Ananda that could be interpreted as an "identifier" is embedded within a file of at least one component of the software as claimed by Applicant.

As per claim 33, Ananda discloses distributing the software via a telephone network and not via computer readable storage medium as claimed.

As per claim 34, Ananda attaches the header module to the application software such that the header module executes without regard to whether an "identifier" is detected. There is no disclosure of detecting an identifier as claimed by Applicant, and no disclosure of performing a process to determine whether an attempted access is authorized based on detection of the identifier as claimed.

As per claim 36, Ananda does not disclose any registration information associated with the user device. The registration information disclosed by Ananda is stored at the central rental facility and associated with a user via the user identification password, not a user device as claimed by Applicant.

As per claim 37, Ananda does not generate at least one authentication code based on the registration information and associate the authentication code with the software as claimed. The authorization verification passwords disclosed by Ananda are independently generated by the user computer and the central rental facility. The messages exchanged include the user computer clock time and the transfer time of the software from the initial transfer to the user computer. Because the transfer time is required to determine the authorization verification password, Ananda does not associate the authentication code with the software as claimed by Applicant.

As per claims 42-43, as described above with reference to claims 18-19 any of the features of Ananda that could be interpreted as an "identifier" are not included in any part of the file name for at least one component of the software as claimed by Applicant.

As per claim 46, Ananda does not disclose associating at least one identifier with the software to designate the software for protection from unauthorized use and then detecting the identifier using the authorized representative installed on or in the user device. Again, if the header module is alleged to anticipate the "identifier", then Ananda does not disclose any other feature that could function as the authorized representative installed on the user device.

As per claim 47, Ananda requires continuous contact with the central rental facility and therefore does not disclose that the software is self activating and self authentication in conjunction with an authorized representative located on or in the user device as claimed.

As per claim 48, Ananda does not disclose an authorized representative entity installed on or in a user device in combination with an identifier distributed with the software that is detected by the authorized representative entity installed on or in the user device to control access to the software in combination with the remote authorized representative entity. As previously described, the authorization verification passwords can not be interpreted as the "identifier" as they are not associated with the software prior to distribution and do not meet various other claim limitations.

As per claim 49, Ananda does not disclose an authorized representative entity installed on or in the user device and does not disclose that it may comprise a computer chip as claimed. The only disclosure in Ananda relative to the central rental facility or the header module is that they are implemented by executable code or software. Similarly, there is no disclosure that the authorized representative may be implemented by an operating system component (claim 51).

As per claim 53, Ananda does not disclose any secondary devices. As such, there is no disclosure for implementing an authorized representative as a driver for a secondary device as claimed.

As per claim 54, Ananda does not disclose registration information associated with a user device and therefore does not disclose comparing registration information associated with a user device to registration information associated with the software as claimed.

As per claims 55-60, the only registration information disclosed by Ananda is contained in the registration database associated with the user via a user identification password entered by the user to gain initial access to the central rental facility database. As described in Applicant's specification, this type of registration information may be easily shared by users to provide unauthorized access to software. In contrast to the registration information disclosed by Ananda, Applicant's claimed invention uses registration information embedded within an authentication code (claim 55), encrypted (claim 56), including hardware information (claim 57), including hardware information associated with a unique user device (claim 58), including a serial number (claim 59), associated with a group of user devise (claim 60), which hinders or prevents such unauthorized use. None of these limitations are anticipated by the registration information disclosed by Ananda.

As per claim 61, there is no disclosure in Ananda that the authorized representative entity is installed by a manufacturer of the user device as claimed.

Similarly, there is no disclosure in Ananda that the authorized representative entity is installed from a computer readable storage medium. The only "installation" that is disclosed in Ananda is transfer of the application program including the header module to the user's computer, which is performed over a telephone network.

With respect to claim 66, Ananda does not prevent the software from being transferred to any device, and does not disclose a second user device. As such, Ananda does not disclose controlling access to the software by preventing the software from being transferred to a second user device. To the contrary, Ananda acknowledges that the software may be copied to a computer readable storage medium from the user's computer, but will be unusable because of the requirement for continuous communication with the central rental facility, and the use of the authorization verification passwords that include the transfer time of the software to the user's original device/computer.

Likewise, as per claims 67-68, there is no disclosure in Ananda of preventing the software from being transferred to, or installed on, the user device if at least one authorized representative is not present as disclosed and claimed by Applicant. The only action taken by Ananda when communication with the central rental facility is lost is termination of the application program.

As per claims 69-70, the only action taken by Ananda when communication with the central rental facility is lost is termination of the application program. Ananda does not disclose preventing the software from executing in the first place, or providing limited access to the software as claimed.

As per claim 73, Ananda does not disclose registration information associated with the user device. Rather, the registration information of Ananda is associated with the user. As such, Ananda does not anticipate generating at least one authentication code based on registration information associated with the user device.

As per claim 75, Ananda does not disclose detecting an identifier associated with the software or controlling access to the software without requiring continuous communication with a remote authorized representative entity. As previously described, the header module disclosed by Ananda executes every time the application program is executed. There is no detection of an identifier to determine whether or not to execute the header software or when to request authentication or authorization.

As per claim 76, Ananda requires continuous communication with the central rental facility for exchange of information to generate the authorization verification passwords. As such, Ananda is not self activating and self authenticating in conjunction with an authorized representative entity located on or in the user device as claimed.

As per claim 77, Ananda does not disclose any feature that could be interpreted as an identifier contained within the filename for the software that triggers an authorization process as disclosed and claimed by Applicant.

As per claim 80, Ananda does not disclose an authorized representative entity installed on the user device as claimed. Rather, the authorized representative entity of Ananda is located at the central rental facility, which communicates with the user device via a telephone network.

As per claims 81-84, Ananda does not disclose registration information associated with a user device. As such, Ananda does not disclose generating an authentication code based on registration information associated with the user device and associating the authentication code with the software as claimed. The registration information disclosed by Ananda is stored in the central rental facility in the registration database and linked to a user (not a user device) via the user identification password entered to gain access to the central facility.

Summary

Applicant's method for securing software using an identifier to indication that protection from unauthorized use is desired as disclosed and claimed in independent claims 1, 23, 46, and 75 includes a number of features that are not disclosed in, and therefore not anticipated by Ananda (US 5,495,411). In addition, numerous features found in dependent claims are not disclosed by Ananda '411. Applicants have made a genuine effort to respond to the Examiner's rejections and advance prosecution of this application. Applicants believe that all substantive and formal requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

No additional fee other than the extension of time fee of $510 and the terminal disclaimer fee of $65 is believed to be due as a result of the filing of this paper. However, please charge any required fees or apply credits to **Deposit Account 50-2841**.

Respectfully submitted:

David S Bir

David S. Bir
Registration No. 38,383

May 21, 2007

Bir Law, PLC
13092 Glasgow Ct.
Plymouth, MI 48170-5241
(734) 927-4531